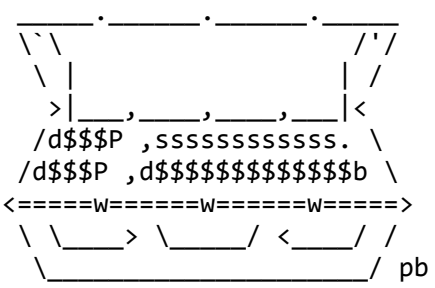
==Phrack Inc.==

Volume 0x0e, Issue 0x44, Phile #0x01 of 0x13

|=---=|
|=-------------------------=[Introduction]=----------------------------=|
|=---=|
|=----------------------=[by the Phrack staff]=-------------------------=|
|=---=|
|=------------------------=[April 14, 2012]=-------------------------=|
|=---=|

"C is quirky, flawed, and an enormous success."
-- Dennis Ritchie

October 2011, a legend has fallen...



Dennis Ritchie, proud father of nothing less than our beloved C language and UNIX operating system, is gone. While the world has been crying over the loss of Steve Jobs, little has been written about Dennis' death. Saying that his inventions influenced the hacking community in a way even he probably never knew is _not_ an exaggeration. Think about it: how many of us became hackers because we discovered C, related bugs or UNIX?

Dennis, the world might not be aware of your unbelievable contribution but we are. Farewell dear friend, may you rest in peace.

-- anonymous bug hunter

-----(Dark Thoughts)-----

Today I woke up thinking about the death of this Chinese little girl [1]. I felt bad. It's true that watching the youtube video was disturbing but something kept hitting my mind. What if the incident had occurred in my country? Would people really have behaved any differently? I have doubts. Just because a video leaked on the Internet people conveniently blamed China, a country both controverted and feared.

What if the modern society in general was tending to slowly become amoral and cold? A proof is that we all watched this video fully aware of its content. Vicious, aren't we? But not only that. We're also fucking cowards. Suddenly discovering that there is a darkness hidden inside the very roots of our society is dramatic. But pretending to ignore the fact that there are countries in this world where atrocious massacres are part of the daily life seems fine.

It was written in the US Declaration of Independence that "We hold these

truths to be self-evident, that all men are created equal [...]". How could that possibly be true? This morning I was at home, healthy, comfortably sitting in front of my computer screen, with a cup of coffee in hand. A few minutes later, I was working (or luxuriously pretending to be) to earn money that I spent in the bar that night with my friends. In the mean time, not so far away, people were killed, raped, mutilated. The truth is that I don't even care when I think about it. This morning I was pretending being concerned for other people, but tonight I don't give a shit anymore.

Something must be wrong.

-- anonymous coward / Phrack

[1] http://www.chinapost.com.tw/china/national-news/2011/10/21/320549/Chinese-girl.htm

-----(Phrack Issue #68)-----

Hello Phrackers! How are you guys doing? We hope well. We hope your latest exploit works reliably (again) and all your bounces are alive and pinging. We also hope you and your friends still are out of prison, or recently came out (wink wink). Us, we're doing good. Looks like we did it again and a new release is here. Ya-hoo.

This release brings you an amazing selection of hacking goodies. We have two papers on applied cryptanalysis by greg and SysK, an area in which we hope to see more submissions for the next issues. We are also thrilled about the return of the Art of Exploitation section. And what a return; we have for you not one, but two detailed papers demonstrating that exploitation is indeed an art form. Speaking of exploitation, did you ever wonder what Firefox, FreeBSD and NetBSD have in common? Read the paper by argp & huku and find out. Are you hacking Windows' farms? Be sure to check the p1ckp0ck3t's novel approach of stealing Active Directory password hashes. Perhaps you prefer malware analysis and identification of malware families; Pouik and G0rfi3ld have written a paper with a focus on Android malware that will satisfy you. Android is quickly becoming the standard mobile platform. I think it's time for an Android/ARM kernel rootkit. Start from dong-hoon you's paper and hack your own. styx^ continues the kernel fun with a paper that updates truff's LKM infection techniques to 2.6.x and 3.x Linux kernels. If for whatever reason you're afraid of messing with your kernels, Crossbower shows you how to create a stealthy userland backdoor without creating new processes or threads.

We also believe that you will find merit with the two main non technical papers of this issue. Both address more or less the same topics, but from two totally different points of view. On one hand, we have an analysis of how the happiness that hacking brings to all of us can and is corrupted by the security industry. One the other, a call to all hackers to take a side between staying true to the spirit of hacking and selling out to the military intelligence industrial complex. Read them, think about them and take a side. Remember, "The hottest places in hell are reserved for those who in times of great moral crisis maintain their neutrality".

Phrack World News is also making a comeback, courtesy of TCLH. In International Scenes we explore Korea and the past of the Greek scene. Loopback has increased and we decided to resurrect Linenoise as we had some tiny but not less interesting submissions. While being eligible for an issue remains hard, submitting for Linenoise may be an easier way for people to share tricks in the next issues.

We are proud to have FX prophiled in this epic issue. As an added gift, FX wrote a eulogy for PH-Neutral, at least in its original form. PH-Neutral, as all great hacker creations, lives on as long as the hackers behind it are fueling it with their passion.

Speaking of hacker passion, this issue re-establishes a long lost connection. Phrack and SummerCon are again bonded on the 25th anniversary of SummerCon! Shmeck and redpantz, representing SummerCon, contribute two papers; a history of the conference from its beginning in 1987 to this year, and of course one of the Art of Exploitation papers.

Believe it or not it was _fucking_ hard to prepare this issue. It's no news that the mentality of the hacking community has changed, but this time we had to face multiple deceptions. It's not the first time, however the quantity makes this event scary. It demonstrates how rotten and corrupted the so-called spirit of some people pretending to be part of the underground has become.

There's a time when you realize that you've lost count of the battles you lost, but you still kinda won enough to keep faith. More importantly, you realize that you still care. Granted, it's not the deep, mystical and life changing moment that movies display -- the huge pile of shit you pushed out of the door just before getting to sleep is still there. It maybe just stinks a little less.

But we care, hell, we really care about Phrack and what it means. It costs time and frustration, many battles lost, it faces the two-point-oh revolution (lots of quality stuff goes into blogs, for immediate consumption) and the money drop by the security industry, but the satisfaction of seeing it out again is huge. Yes, we care.

And that's not just because we're a bunch of old farts that stay attached to the past. We care because it's a constant, maybe feeble but constant, heartbeat of that world, that community that we grew up and now live in. You know, that little thing called 'the Underground' that we are proud and honored to somehow, in part, represent.

We've heard from many corners that 'the Underground' is dead. We'd love to hear those people describe what the Underground is, then. Sure, things change, evolve. Laws, computing power, money invested, political links, technology, every piece moves fast and reshapes the landscape. But if you're reading these lines today, if you've just finished a 36-hour coding, hacking marathon, you're keeping it alive.

So thank you, for that. Thank you to the authors for finding the time of sharing their knowledge. Thank you to anyone that setups a new connection. Thank you to whomever fights for information and freedom. Thanks crews.

Happy hacking, Phrackers.
You guys are the BEST heartbeat in the world.

-- the Phrack staff

```
 |_|     |_|   |_|     |_|______|\______)_|  \_)    |__||_|  \____/ \_____/

                - By the community, for the community. -

 $ cat p68/index.txt

 <-------------------------( Table of Contents )------------------------->

  0x01  Introduction ..................................... Phrack Staff

  0x02  Phrack Prophile on FX ............................ Phrack Staff

  0x03  Phrack World News ................................ TCLH

  0x04  Linenoise ........................................ various

  0x05  Loopback ......................................... Phrack Staff

  0x06  Android Linux Kernel Rootkit ..................... dong-hoon you

  0x07  Happy Hacking .................................... Anonymous

  0x08  Practical cracking of white-box implementations ... SysK

  0x09  Single Process Parasite .......................... Crossbower

  0x0a  Pseudomonarchia jemallocum ....................... argp & huku

  0x0b  Infecting loadable kernel modules ................ styx^

  0x0c  The Art of Exploitation:
        MS IIS 7.5 Remote Heap Overflow .................. redpantz

  0x0d  The Art of Exploitation:
        Exploiting VLC, a jemalloc case study ............ huku & argp

  0x0e  Secure Function Evaluation vs. Deniability in OTR
        and similar protocols ............................ greg

  0x0f  Similarities for Fun and Profit .................. Pouik & G0rfi3ld

  0x10  Lines in the Sand: Which Side Are You On in the
        Hacker Class War ................................. Anonymous

  0x11  Abusing Netlogon to steal an Active Directory's
        secrets .......................................... the p1ckp0ck3t

  0x12  25 Years of SummerCon ............................ Shmeck

  0x13  International Scenes ............................. various

 <---------------------------------------------------------------------->


                    -----( GreetZ for issue #68 )-----

     - FX:                          epicness personified
     - herm1t:                      you have our support
     - TCLH:                        for everything
```

```
    - x82:                          deepest apologies for the 1 year wait
    - anonymous authors:            best part of this issue
    - sysk:                         keep submitting man!
    - redpantz & Shmeck:            Phrack and SummerCon bonded again
    - greg:                         schooling Alice and Bob
    - Crossbower:                   parasite zoologist
    - the p1ckp0ck3t:               be wary or he will get your hashes
    - huku & argp:                  the scourge of memory allocators
    - styx^:                        yes we are hardcore reviewers
    - Pouik & G0rfi3ld:             who the hell is G0rfi3ld??? ;>
    - scene phile writers:          you have big balls guyz
    - linenoise writers:            Eva you're soooooooo cute :3
    - our generous hoster:          a contribution not forgotten ;)
    - z4ppy, ender:                 external reviews are paid in beers
    - b3n:                          too bad we didn't use your stuff
    - No greetz, no thankz to:      you know who you are :<

       And of course many thanks to the loopback contributors :')


                  -----( Phrack Magazine's policy )-----

 phrack:~# head -n 22 /usr/include/std-disclaimer.h
 /*
  *  All information in Phrack Magazine is, to the best of the ability of
  *  the editors and contributors, truthful and accurate.  When possible,
  *  all facts are checked, all code is compiled.  However, we are not
  *  omniscient (hell, we don't even get paid).  It is entirely possible
  *  something contained within this publication is incorrect in some way.
  *  If this is the case, please drop us some email so that we can correct
  *  it in a future issue.
  *
  *
  *  Also, keep in mind that Phrack Magazine accepts no responsibility for
  *  the entirely stupid (or illegal) things people may do with the
  *  information contained herein.  Phrack is a compendium of knowledge,
  *  wisdom, wit, and sass.  We neither advocate, condone nor participate
  *  in any sort of illicit behavior.  But we will sit back and watch.
  *
  *
  *  Lastly, it bears mentioning that the opinions that may be expressed in
  *  the articles of Phrack Magazine are intellectual property of their
  *  authors.
  *  These opinions do not necessarily represent those of the Phrack Staff.
  */

                  -----( Contact Phrack Magazine )-----


            <  Editors           : staff[at]phrack{dot}org   >
            >  Submissions       : staff[at]phrack{dot}org   <
            <  Commentary        : loopback[@]phrack{dot}org >
            >  Phrack World News : pwned[at]phrack{dot}org   <


    Submissions may be encrypted with the following PGP key:
    (Hint: Always use the PGP key from the latest issue)


 -----BEGIN PGP PUBLIC KEY BLOCK-----
 Version: PHRACK
```

```
mQGiBEucoWIRBACFnpCCYMYBX0ygl3LrH+WWMl/g6WZxxwLM2IT65gXCuvOEbLHR
/OdZ5T7Z6sO4O5b0EWkk5pa1Z8egNp44+Fn+ExI78cv7ML9ffw1WEAS+raQwvN2w
0WUsfztWHZqPf4HMefX92pv+1kVcio/b0aRT5lRbvD7IdYLrtYb0V7RYGwCgi6Or
dJ5iN+YVDMx8lkUICI8kPxcD/1aHZqCzFx7lI//4OtZQN0ndP1OEH+C7GDfYWi4P
DcLNlF812h1qyJf3QCs93PQR+fu7XWAIyyo5rLHpFfuU29ZZH1Oe0VR6pLJTas2Z
zXNdU48Bhj1uf4Xv0NaAYlQ5ffIJ4a37uIKYRn28sOwH/7P8VGD7K7EZn3MMyewo
aPPsA/4ylQtKkaPB9iTKUlimy5ZZorPwzhNliEbIanCGfePgPz02QMG8gnId40/o
luE0YK1GnUbIMOb6LzI2A5EuQxzGrWzDGOM3uLDLzJtBCg8oKFrUoRVu1dnPEqc/
NQzRYjRK8R8DoDa/QZgyn19pXx4oQ3tAldI4dAQ022ajUhEoobQfUGhyYWNrIFN0
YWZmIDxzdGFmZkBwaHJhY2sub3JnPohgBBMRAgAgBQJLnKFiAhsDBgsJCAcDAgQV
AggDBBYCAwECHgECF4AACgkQxgxUfYgthE7RagCeL/XirVrcUzgKBrJGcvo0xjIE
YlkAoIBqC2GuYJrXxPO/KaJtXglJjd7zuQQNBEucoWIQEADrU+2GAZbWbTElblRp
/MyoUNHm0gxOo7afqVdQe8epub/waQD1bnE+VucI7ncmQWUdD0qkkyzaXlFDlvId
LYh/dMu4/h+nTyuCLNqoycqvf1k8Dax6QOADq0BZlM5lGTL6VOBnCitWCvgYCmLO
aPO1bacJlNx0/cpWKe+YELlZss7Q+o4SBvDOyX8B78eEs62dbRAudubFQ/tjQd3z
cXZOSli9Du9DAa2vzk8tq1c6RAs0NY4KxBu+6VW/lxvGt3iNRlFQAdya6Kx3fhog
zVjkt3OOgNDJ6u/9zYbMbtjtoFqSIJDR4DhZ9NbS57nuTkJqh0GDVOtxfKcc8QxH
wyYiH47M9znHFtHHvT0PzGc2Fl8s3EUFvlXZUW3ikcFbkyqTgnseqv5k9YQ8FDHX
IvBVpj8nqLi3CBADy8z2gy5r4TryV3sfOlTT40r0GtiG3Weeb0wuMj5+hr303zgN
/aH+ps8JvL0TeyXjsDMcTCF1fHSIxPJouSWjOkFMrumAg/rikdn3+dPCCowcLKvQ
isYC60yKEhcYvUDiKKzXrGyM/38Kp/73RA9ZLQ3VjCSX550UCU46hF6u6Qzbd5Jk
T8WesPYqz4jpPzlF1MbaVki4+g5myTR8y1IIarX08mk6l+1YZyjjzmlhKyhdaIiI
QY4uv3EYYFDHiyd0/3ZBfkz62wADBQ//bVf698IFhoLHeCG3USyl/rHyjVUatsCx
ZCwPlWEGzR+RP3XdqwoeFZNA4hXYy3Qr1vJSytbCRDYOK2Rp3Eos1Gncqp3KbUhQ
ZRBxGNbhskZ7VHOvBHIIZ7QU3TDnWLDlWs9oha8zv9XWEmaBmCjBtmRwunphwdv2
O7JpqLbW45l/WAas6CuRi+VxXllQPM2nKX9JwzyWlvnU3QayO+JJwH5bfeW0Wz53
wqMBJz9hvVaClfAzwEnPnWQxxgA6j7S9AuEv7NRLZsC6nHyGwB7vFfL4dCKt4cer
gYOk5RjhHVNuLJSLhVWRfcxymPRKg07harb9adrPcjJ7fCKXN1oPCcacG0O6vcTb
k58MTzs3CShJ58iqVczU6ssGiVNFmfnTrYiHXXvo/+36c+TizwoXJD7CNGDc+8C0
IxKsZbxgvpFuyRRwrzr3PpecY0I2cWZ7wN3WtFZkDi5OtsIKTXHOozmddhAwxqGK
eURB/yI/4L7t2Kh2EaVOyRbXNa4hwPbqbFiofihjKQ1fFsYCUUW0CAOaXu14QrrC
IepRMQ2tabrYCfyNuLL3JwUFKinXs6SrFcSiWkr9Cpay7Ozx5QosV8YKpn6ojejE
H3Xc0RNF/wjYczOSA6547AzrnS8jkVTV2WIJ5g1ExvSxIozlHU5Dcyn5faftz++y
ZMHT0Ds1FMGISQQYEQIACQUCS5yhYgIbDAAKCRDGDFR9iC2ETsN0AJ9D3ArYTLnd
lvUoDsu23bN4bf7gHwCfUGDsUSAWE/G7xQaBuB50qXecJPo=
=cK7U
-----END PGP PUBLIC KEY BLOCK-----

                              -----( EOF )-----
```